ZKTeco®

Security and Time Management Solutions



Manual de Usuario

Versión 1.2
Date: AGOSTO
2013

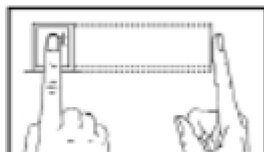
Tabla de contenidos

1. Instrucciones

1.1 Posición del dedo

No se recomienda el pulgar y el meñique (ya que suelen ser torpes en la pantalla de reconocimiento de huellas dactilares) el dedo índice, el dedo medio y el anular son los dedos recomendados.

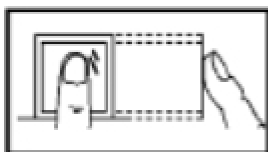
1. FORMA APROPIADA DE COLOCAR EL DEDO



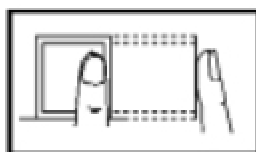
EL DEDO DEBE COLOCARSE JUSTO EL CENTRO DEL SENSOR DACTILAR HUELLA COMPLETA

2. FORMA INAPROPIADA DE COLOCAR EL DEDO

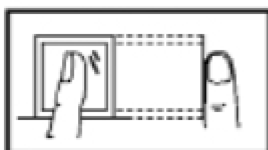
HUELLA INCOMPLETA



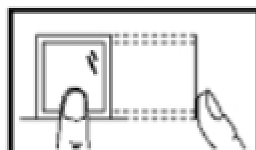
FUERA DEL CENTRO



DE COSTADO



FUERA DEL CENTRO



Por favor, registrarse y verificar su huella digital utilizando el modo adecuado de colocación de los dedos. No vamos a ser responsables de las consecuencias que se deriven de la degradación del rendimiento de verificación debido a las operaciones de usuario inapropiadas. Nos reservamos el derecho de la interpretación final y la revisión de este documento.

1.2 Instrucciones para pasar la tarjeta

Este producto se suministra con un RFID sin contacto integrado (125 MHz), lector de tarjetas de módulo. Al ofrecer múltiples modos de verificación tales como huella digital, tarjeta de RF y de huella digital + tarjeta de verificación de RF, este dispositivo puede satisfacer las necesidades de usuarios diversos.

Deslice su tarjeta a través de la zona del sensor después escuchará la voz una vez que el sistema la ha detectado. Para el área de tarjeta, consulte 2.2 Aspecto del producto.

1.3 Precauciones

Protege el dispositivo de la luz solar directa o luz fuerte, esto afecta en gran medida la recogida de huellas dactilares y conduce a un error de comprobación de huellas. Se recomienda utilizar el dispositivo bajo una temperatura de 0-50 ° C a fin de lograr el rendimiento óptimo. En el caso de la exposición del dispositivo a la intemperie durante largos periodos de tiempo, se recomienda la adopción de sombrilla y disipación de calor ya que la exposición excesiva a alta o baja temperatura puede ralentizar el funcionamiento del dispositivo y provocar alta tasa de falso rechazo (FRR).

Cuando instale el dispositivo conecte el cable de alimentación después de conectar el resto de cables. Si el dispositivo no funciona correctamente, asegúrese de apagar la fuente de alimentación antes de realizar las inspecciones necesarias. Tenga en cuenta que cualquier trabajo en tensión puede provocar daños en el dispositivo lo cual no será cubierto por la garantía del equipo.

Para las cuestiones que no se tratan en este documento, por favor consulte los materiales relacionados, incluyendo la guía de instalación, manual de usuario del software de control de acceso.

Summario

* porfavor asegurese de colocar el dedo correctamente en el lector

* Tarjeta RFID

* No instale directamente a la luz del sol

* Temp 0 - 50°C

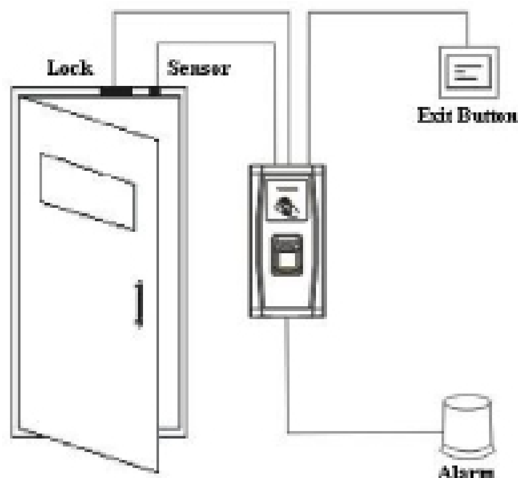
* Primero conecte todos los cables antes de la alimentación

* Apague la unidad antes de dar mantenimiento

2. Introducción del equipo

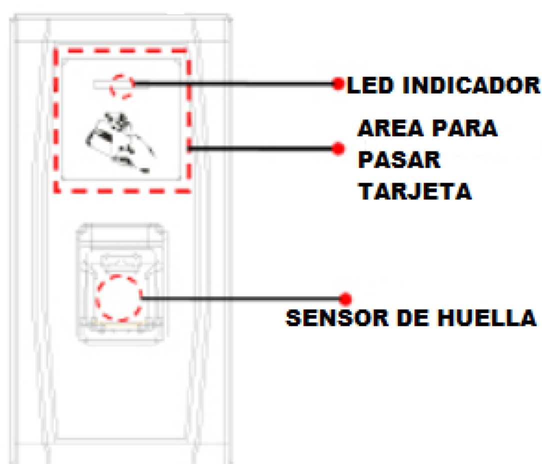
2.1 Vista de las funciones del equipo

Como un dispositivo integrado de huella digital y de control de acceso, nuestro producto se puede conectar, ya sea con una cerradura electrónica o un controlador de acceso. Este dispositivo cuenta con operaciones simples y flexibles y admite el uso de tarjetas de gestión. Con una tarjeta de gestión, puede realizar funciones tales como la inscripción sin conexión, eliminación y U-disco de gestión. La voz le guiará a través de todas las operaciones sin la pantalla. Este dispositivo le permite conectar un teclado externo y ofrece múltiples modos de operación. Es compatible con la función de control de acceso para una gestión de la seguridad. Es compatible con múltiples modos de comunicación. El U-disco cuenta con operaciones sencillas y convenientes. Con un diseño compacto y simple, este dispositivo permite a los usuarios conectar varios dispositivos a través de un PC y realizar la supervisión en tiempo real.



2.2 Apariencia del equipo

vista frontal:



- **LEDs indicadores**: Los LEDs indicadores se utilizan para mostrar los resultados de operación de dispositivos y los estados a excepción que se definen de la siguiente manera:
- **Comunicación**: si una operación es completada el indicador verde se iluminara por un segundo si no se iluminara el rojo por un segundo
- **Estado de Registro**: El LED verde parpadea tres veces cada tres segundos.
- Borrar un solo usuario: El LED rojo parpadea tres veces cada segundo
- Estado de verificación: El LED verde parpadea una vez cada dos segundos.
- **Á**rea para pasar la tarjeta: Se refiere a la zona en el cuadro de línea roja se muestras en la figura
- **S**ensor de huella: Usado para registrar y ubicar usuarios.

Sumario

*Se puede conectar a un electro iman de control de acceso

*Use la tarjeta administradora para agregar o borrar usuarios

* Usb compatible para bajar y subir usuarios

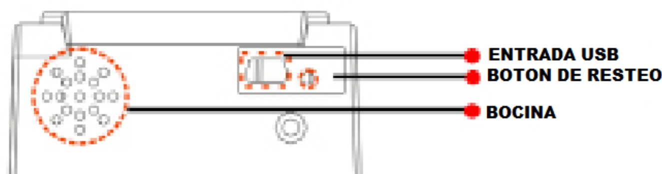
* Diagrama de posibilidades de conexion

* Areas importantes en MA300.

* los LEDS indicadores son. para una facil manipulacion

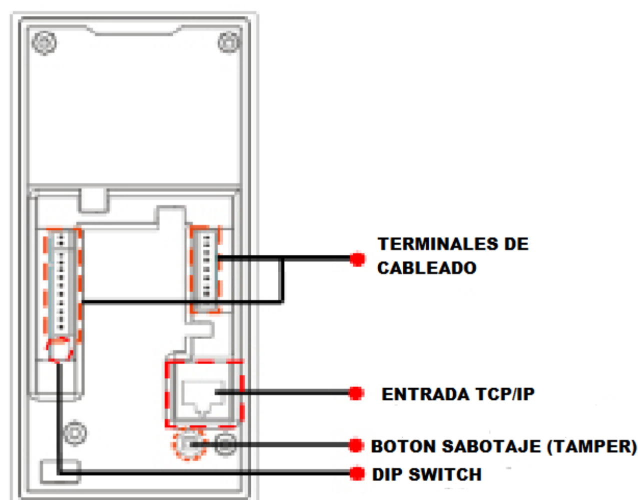
*Tome nota del area para pasar la tarjeta

Vista desde abajo



- Entrada **USB** Se usa para conectar una USB o un teclado exterior.
- **Botón** de reset: Para reiniciar el equipo.
- Bocina: Esta será usada para corroborar las acciónes del equipo como acceso correcto o negado

Vista trasera



- Cableado de equipo: se muestra como conectar con el botón o alimentación
- **TCP/IP**: La interfaz de TCP / IP se conecta a un PC a través de un cable de red (para la conexión en cola por favor consulte la guía de instalación.
- **Tamper Switch**: Se utiliza para generar una alarma de sabotaje. Para obtener más información, consulte 3.6 alarma de sabotaje
- **DIP Switch**: El interruptor DIP tiene cuatro pines numerados 1, 2, 3 y 4. En la comunicación RS485 de utilizan 1, 2 a 3 ª para establecer el número de dispositivo y el cuarto pin se utiliza para seleccionar el estado de la resistencia terminal.

2.3 Usando un teclado USB externo

Para facilitar las operaciones del dispositivo, puede conectar el dispositivo con un teclado USB (comprado por los usuarios) y llevar a cabo operaciones tales como la incorporación de usuarios, eliminación y restauración de valores de fábrica, sobre todo cuando se especifica la ID de usuario durante la inscripción del usuario y eliminación.

Summario

* Tome nota del puerto USB y el boton de reset

* Config de DIP switch:

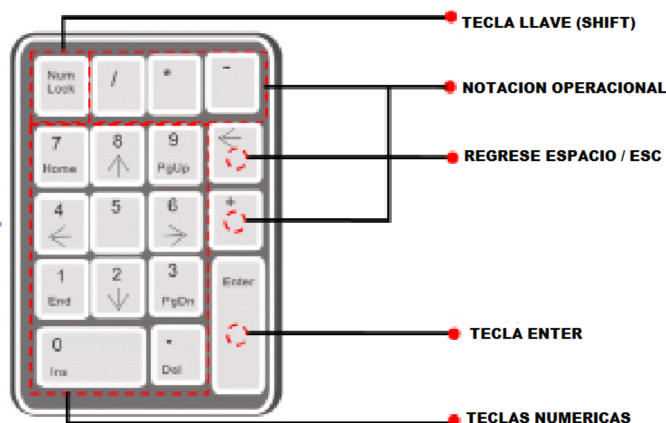
** cuatro pins 1,2,3 & 4

*** Pins 1,2 & 3 - configuran el numero del equipo

*** Pin 4 - selecciona el estado de resistencia de la terminal.

* Con el teclado USB incluso puede borrar y agregar usuarios

Teclado USB:



Un teclado USB externo se muestra arriba (consulte al producto real):

NumLock es una tecla de modo del teclado numérico. Se activa de forma predeterminada. Si está activado, el indicador LED está encendido. Cuando el dispositivo está conectado a un teclado externo, sólo puede utilizar las teclas numéricas, la tecla "Retroceso" y la tecla "Enter" en el estado activado Bloq Num.

2.4 Estado de verificación

Estado de verificación: Cuando el dispositivo está encendido, entrará en el estado de verificación si una tarjeta de gestión se ha inscrito antes o vuelve de otros estados.
En el estado de verificación todos los usuarios están autorizados para verificar su identidad y desbloquear la puerta (el administrador que lleva una tarjeta de gestión sólo puede abrir la puerta mediante el uso de su huella digital (s) previamente inscrita), el administrador puede realizar operaciones como usuario inscripción / eliminación, gestión del USB y el funcionamiento del teclado.

2.5 Gestionando la tarjeta (M-card)

Los usuarios de dispositivos se clasifican en administradores y usuarios comunes.

Administradores: Se permite un administrador para realizar todas las operaciones, incluido el usuario, la matrícula, supresión de todos los usuarios (excepto a sí mismo / a sí misma) y gestión de USB. Los privilegios de los administradores de dispositivos se implementan a través de las tarjetas de gestión.
Usuarios **Comunes** Los usuarios normales sólo pueden verificar su identidad y abrir la puerta.
Una tarjeta de gestión es una tarjeta especial asignada a un administrador. Cada equipo debe tener al menos una tarjeta de gestión de matrícula. Si no hay ninguna tarjeta de gestión inscrita no se puede realizar ninguna operación y el sistema generará un mensaje de voz: "Por favor, registrar la tarjeta de administrador". Puede aplicar diferentes funciones al deslizar una tarjeta de gestión de tiempos diferentes en una fila:

- Al pasar la tarjeta de gestión una vez , se puede entrar en el estado de matricular un solo usuario.
- Al pasar la tarjeta de gestión cinco veces seguidas, puede entrar en el modo de eliminación de usuarios.
- USB **conectada:**
- Al pasar la tarjeta de gestión de una vez, se puede entrar en el estado de gestión de USB.
- Un Teclado externo esta conectado:
- Al pasar la tarjeta de gestión de una vez, puede activar el teclado externo.

Summario

* Teclado USB

* NUMLOCK es alternar el teclado numérico.

* Cuando se conecte solo use :

**teclas Numéricas

**Barra espaciadora

**La tecla ENTER

* Administrador tiene acceso completo a gestion del sistema.

* Los usuarios sólo pueden verificar la identidad y desbloquear

* pase su tarjeta una vez para registrar usuarios
* Pase la tarjeta 5 veces para el modo de borrado

* Pase la tarjeta para la gestion de USB

* Pase la tarjeta una vez para el uso del teclado.

Pases de tarjetas consecutivos: Golpes consecutivos significa el intervalo entre dos golpes consecutivos a menos de 5 segundos.

Las tarjetas de administración se pueden eliminar a través de "Clear All" función del teclado o a través de software antes de ser eliminados como tarjetas de identificación común. Para obtener más detalles, consulte el manual de usuario del software de control de acceso.

La FP de administrador (el que posee tarjeta de administración) puede ser inscrito a través de software o inscripción del teclado.

Un equipo sin tarjeta de administrador: si tiene la contraseña de teclado, puede activar el teclado externo y matricularse

Nota: Los usuarios que llevan tarjetas de administración sólo pueden verificar su identidad y desbloquear el uso de sus huellas digitales previamente inscritos.

2.6 Password del sistema

La clave del sistema es una contraseña que se utiliza para mejorar la seguridad de los datos del dispositivo en TCP / IP o comunicaciones RS485.

Nota: El password puede ser modificado o borrado desde el software de control de acceso

2.7 Tiempo de operación expirado

Hay 30 segundos antes de los tiempos de operación terminada, La voz le avisará cada 10 segundos durante 3 veces si no hay ninguna operación apropiada. Después de estos 30 segundos, el sistema se regresa al modo de verificación con el comando: "Tiempo expirado. El sistema vuelve al estado de verificación" .

Note: usted podrá configurar este tiempo desde el software de control de acceso.

3.Operación del equipo

3.1 Tarjeta administradora

3.1.1 Enrolar una tarjeta administradora

Para registrar una tarjeta de gestión, por favor haga lo siguiente:

1. El dispositivo se detecta automáticamente si existe una tarjeta de gestión.

2. Después de que el equipo diga la voz "por favor registre la tarjeta de administrador", puede pasar la tarjeta por el área indicada para registro.
3. Si esto falla el sistema dirá el siguiente comando "El número de tarjeta esta repetido" y regresa al paso 3; agregar tarjeta de administrador, el sistema generará el comando La verificación ha sido completada el sistema vuelve al modo de verificación".

Nota: el sistema vuelve al modo de verificación si en cualquier operación no recibe respuesta después de 30 segundos y solo lo hará si presenta la tarjeta de administrador después de reiniciar el equipo.

Summario

* Menos de 5 segundos entre golpes consecutivos.

* M-card se puede eliminar a través de "Clear All" función a través de software.

* Contraseña del sistema configurada a través del software de control de acceso.

* Por default 30 segundos

* 3 comandos de voz de advertencia

* Tome nota de los pasos de como agregar una tarjeta de administrador.

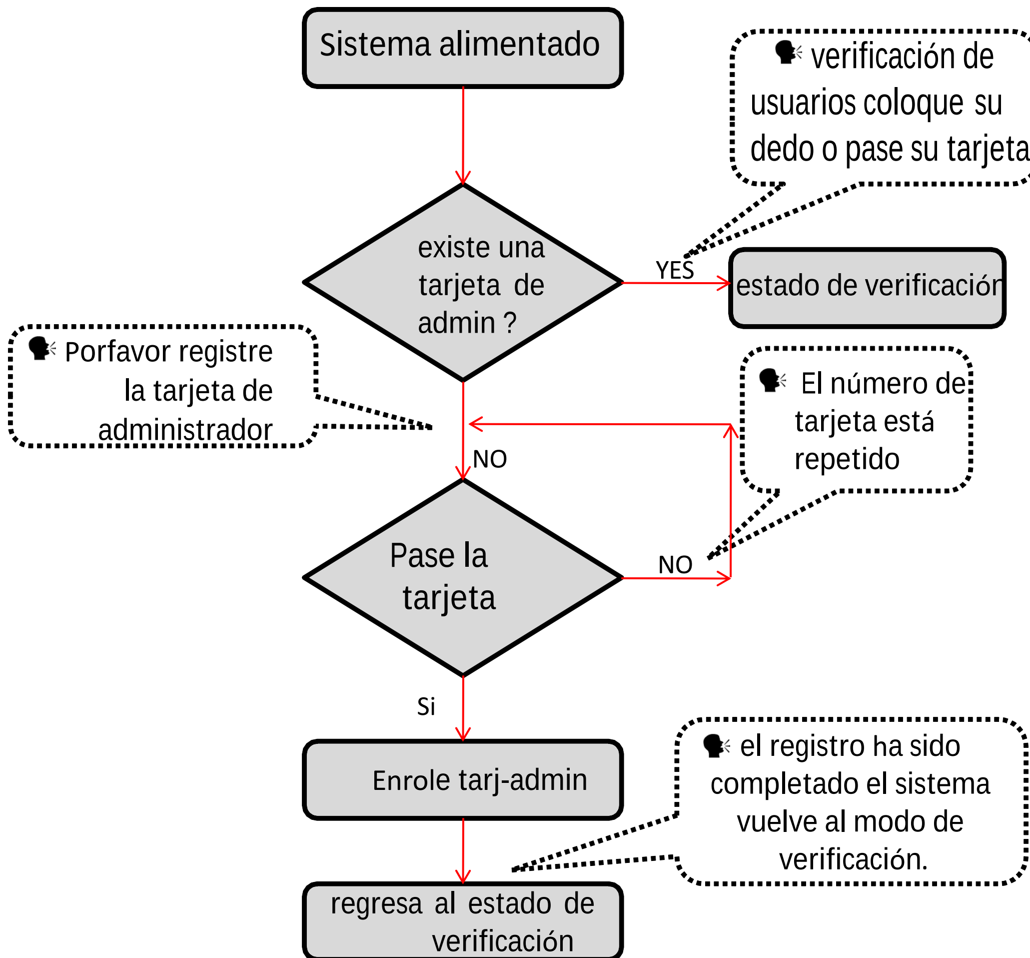
*el sistema la detecta automatico

** Falla de detección: el sistema avisara en la falla de deteccion.

**pasar tarjeta

** Registro completo

Tabla de como enrolar una tarjeta de administrador:



3.1.2 Agregue un usuario ordinario

El modo para que usted pueda entrar en el estado de enrolar es mediante el uso de la tarjeta administradora se llama el modo de gestión de usuarios En este modo, sólo se puede inscribir a un usuario. Cuando se inscribe un nuevo usuario el sistema asigna automáticamente un ID para el usuario. Por otra parte, también se puede utilizar el modo de inscripción con el teclado externo (Para más detalles, consulte 3.2.2 agregar usuario con el teclado) para implementar la incorporación de usuarios con un ID concreto.

En ambos de estos modos de inscripción, pueden inscribirse nuevos usuarios. Se permite a cada usuario que registre 10 huellas digitales y una tarjeta de verificación como máximo.

Para agregar un usuario siga estos pasos:

1. E el sistema entra al modo de registro de usuarios después de pasar una tarjeta de gestión una vez (después del estado de inscripción, deslizar una tarjeta de gestión una vez para que se devuelva el aparato al estado de verificación).
2. Después de que el sistema genera el mensaje de voz: "Registro de usuarios Por favor coloque el dedo o pase su tarjeta ", puede iniciar la incorporación de usuarios. Hay los tres casos siguientes:





Summario

* Por favor siga los pasos y comandos de voz de la izquierda para enrolar una tarjeta

* modo de enrolar tarjetas de administrador

* 10x huellas por usuario y 1 tarjeta RFID

* modo de verificación pase su tarjeta para registrar un usuario

* Estado de agregar - pase la tarjeta de admin para regresar al modo de verificación

* siga los comandos

1. Pase la tarjeta primero

- Cuando pase su tarjeta de admin y tenga éxito en agregar a un usuario el dispositivo generará un mensaje de voz: "Número del usuario. ** El registro es exitoso" (** se refiere al ID que se asigna automáticamente al usuario por el sistema lo mismo más adelante) y se puede continuar con el siguiente paso, si usted pasa una tarjeta de admin el sistema genera el mensaje de voz: "Número del usuario ** registrado. Por favor coloque el dedo" y entrará en el estado de inscripción de usuario especificado
- Después de que el dispositivo genere el mensaje de voz: "Registro. Por favor coloque su dedo ", el sistema entrara al estado específico de registro de huellas dactilares. Pulse el mismo dedo en el sensor tres veces después de las instrucciones de voz.
- Si el registro de huellas dactilares tiene éxito el sistema genera el mensaje de voz: "Registro exitoso Por favor, pulse el dedo" y entrara directamente al siguiente estado de inscripción de huellas digitales si el registro de huella falla el sistema genera el mensaje de voz: "Huella duplicada "y deberá repetir el paso anterior.
- El sistema volverá automáticamente al estado de verificación al registrar 10 dedos y la tarjeta de administración a sido pasada

2. Coloque el dedo primero

- Pulse el mismo dedo sobre el sensor tres veces después de las instrucciones de voz . Si el registro de huellas dactilares tiene éxito, el sistema genera el mensaje de voz: "Número del usuario. *x* El registro es exitoso "y se puede continuar con el paso b, si la huella digital no se ha inscrito antes, el sistema genera el mensaje de voz: "Usuario no registrado, por favor presione el dedo o pase la tarjeta " y entrará en el estado de inscripción de usuario especificado .
- Después de generar el comando: "Registro por favor coloque el dedo o pase su tarjeta'', el sistema introduce la información del usuario especificado a la espera para que usted pase su nueva tarjeta de identificación o presione su dedo.
- Si la inscripción de la tarjeta de identificación tiene éxito, el sistema genera el mensaje de voz: "El registro se completó Por favor, pulse el dedo" y entra directamente en el estado de gestión de huellas digitales, si se presiona con un dedo que no se inscribió antes y tiene éxito en la matrícula de este dedo, el sistema genera el indicador de voz: "El registro es exitoso. Por favor, pulse el dedo o pase la tarjeta" y usted puede seguir registrando nuevas huellas digitales y tarjetas. Después de registrar 10 huellas dactilares, el sistema generará el indicador de voz: "Por favor pase la tarjeta" para inscribir a su tarjeta de identificación si su tarjeta de identificación no está inscrita.
- El sistema vuelve automáticamente al estado de verificación cuando se inscriben 10 dedos y la tarjeta de administrador.

3. Si ya se le ha asignado un número de usuario:

- Inscriba huella (s) cuando ya se ha pasado tarjeta
- Después de que pase la tarjeta enrolada dirá el siguiente comando:

  "Número de usuario *x*. Registrado. Por favor, pulse el dedo" y entrará en el estado de registro de huellas dactilares.
- Pulse el mismo dedo sobre el sensor tres veces después de las instrucciones de voz mediante la adopción de la colocación de huellas digitales correctas. Si el registro de huellas dactilares tiene éxito, el sistema genera el mensaje de voz: "Número del usuario. *x* El registro es exitoso" y se prepara para la matrícula de la próxima huella digital.
- El sistema vuelve automáticamente al estado de verificación cuando se inscriben 10 dedos y la tarjeta de administrador

✍ **Nota**: La huella de administrador no puede ser inscrita por esta modalidad

Summario

*porfavor siga los pasos y comandos que aparecen en la izquierda

* coloque su dedo tres veces y siga los comandos

*si la regitracion falla vovera al modo de registro e intentelo de nuevo

* el sistema volvera al modo de verificacion despues de registrar 10 dedos o pasar la tarjeta de administrador

* debe presionar el mismo dedo tres veces para enrrolar

* los usuarios pueden enrrolar 10 dedos en una trajeta.

* puede detener los procesos solo pasando la tarjeta de administradora.

* siga los pasos para como enrrolar una huella despues una tarjeta.

* si un usuario sobreescribira una huella dactilar

3.1.3 Enrolar tarjeta y huella **(s)** cuando ya este enrolada una huella **(s)**

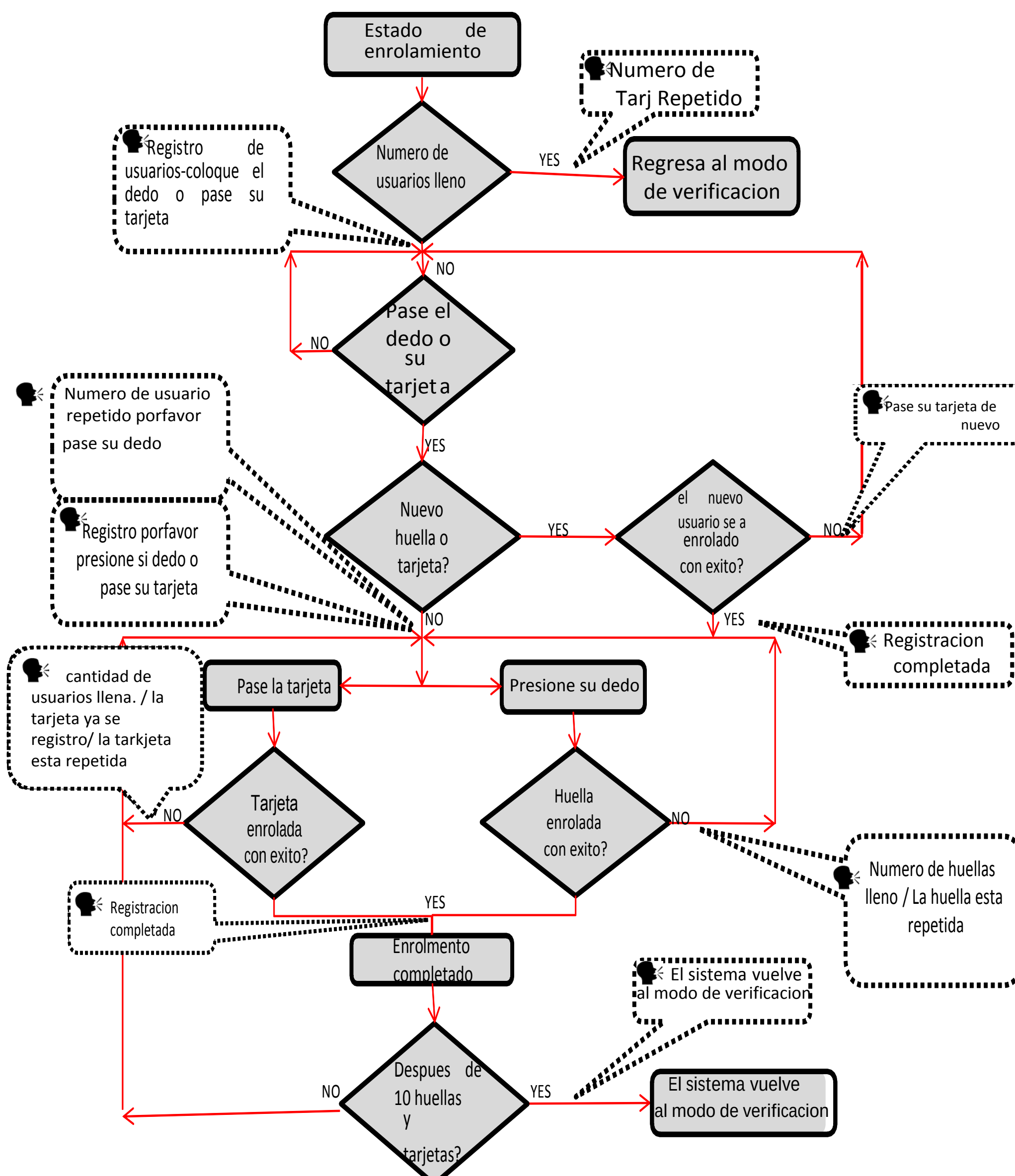
- Presione el dedo con la huella digital que ya inscribieron tres veces siguiendo las indicaciones de voz, que usted este identificado como la misma persona en cada uno de los intentos de verificación.
- Después generará el mensaje de voz "número de usuario*. Registrarse Por favor, pulse el dedo"
- Si la inscripción de la tarjeta de identificación tiene éxito, el sistema genera el comando "Registro completado por favor presione el dedo." Y entrará en el estado de gestión de huellas dactilares si presiona un dedo que no se enrolo antes y logra el registro de este dedo, el sistema generará el comando: "Registro completo. Por favor, pulse el dedo o pase la tarjeta" y usted puede seguir registrando nuevas huellas digitales o tarjetas. Después de que se hayan grabado 10 huellas el sistema pedira volver a enrolar una tarjeta de administrador.
- El sistema volverá al modo de verificación un vez que 10 huellas y una tarjeta de administrador sean grabadas

Summario

* Presione su dedo tres veces y siga las indicaciones

*Siga las indicaciones de voz

*Despues de 10 huellas el sistema volvera al modo de verificacion



3.1.4 Borrar a un usuario

Borrar un usuario usando la tarjeta de administrador es el Modo de borrado de un usuario simple y borrando un usuario con el teclado exterior es Modo de borrado de un usuario especifico . (Ver 3.2.3 borre un usuario especificado).

Pasos para borrar un usuario simple:

- En estado de verificación, pase su tarjeta de administrador 5 veces consecutivas para entrar al modo de borrado de usuario (pase su tarjeta una vez más y voleverá al modo de verificación).



- El sistema genera un comando de voz Borrado de usuarios. por favor presione su dedo o pase su tarjeta."
- Presione su dedo dentro del sensor o pase su tarjeta.
- Presione el dedo del usuario que desea borrar.

  Pulse uno de sus dedos registrados correctamente en el sensor. Si la verificación tiene éxito, el sistema generará el indicador de voz: "Número del usuario. ** Borrado con éxito. Eliminar usuarios. Por favor, pulse el dedo o pase su tarjeta." (** Indica el número de identificación del usuario) y volverá automáticamente al estado de borrado. Si la verificación falla, el sistema generará el indicador de voz: "Por favor, pase de nuevo:
- Pase su tarjeta sobre el lector para borrar un usuario.
- Pase una tarjeta registrada sobre el lector si la verificación se completa el sistema dirá el comando de voz: Número de usuario**. borrado con éxito. borrado de usuarios. presione su dedo o pase su tarjeta." y automáticamente regresara al modo de borrado. si la verificación falla, el sistema generara el comando de voz: "Por favor pase su tarjeta de nuevo."
- Si pasa su tarjeta una vez más o se tarda en el tiempo de operación, el sistema volverá al modo de verificación

Nota: En el modo de borrado de un solo usuario simple las tarjetas de administración no se pueden eliminar porque al pasar la tarjeta de administración se regresara al sistema o modo de verificación.

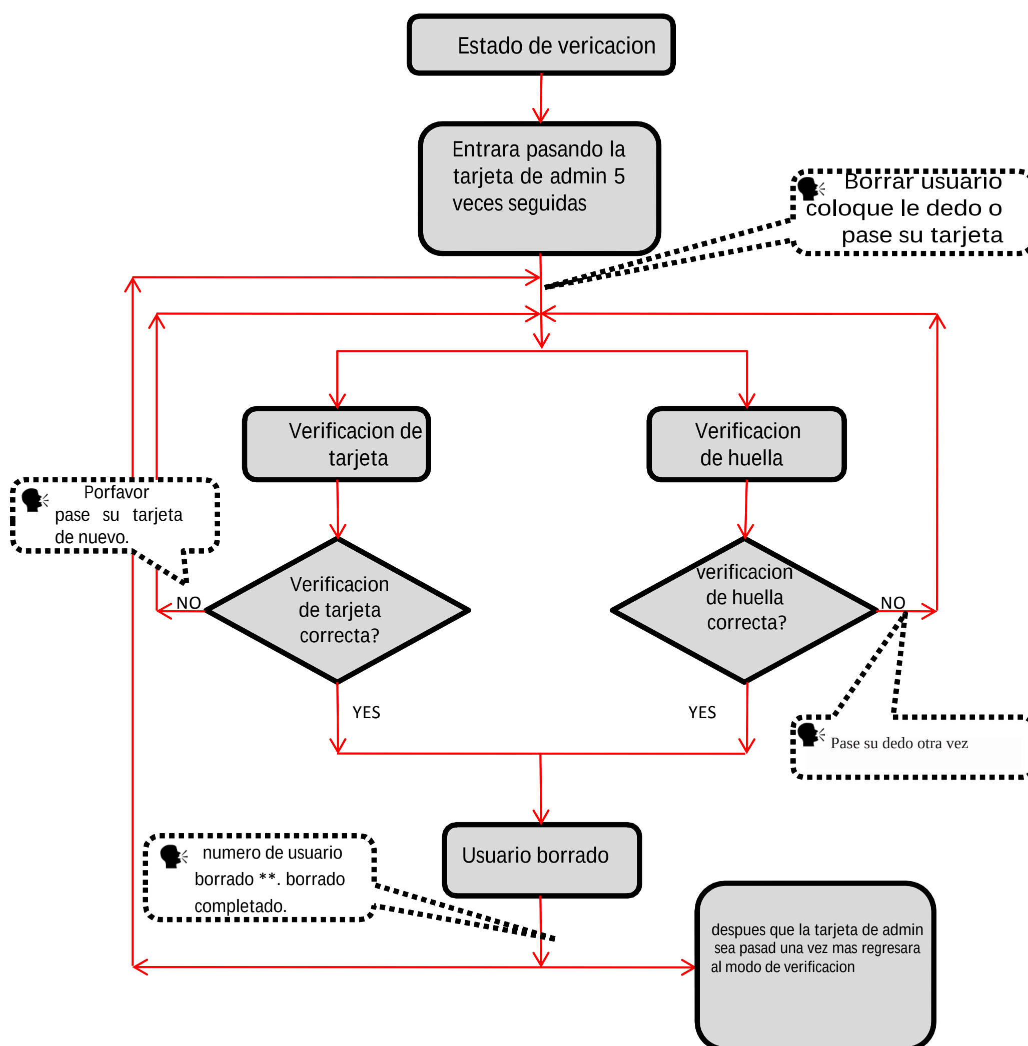
Sumario

* Borrar un usuario del modo normal

* borrar un usuario con el teclado exterior

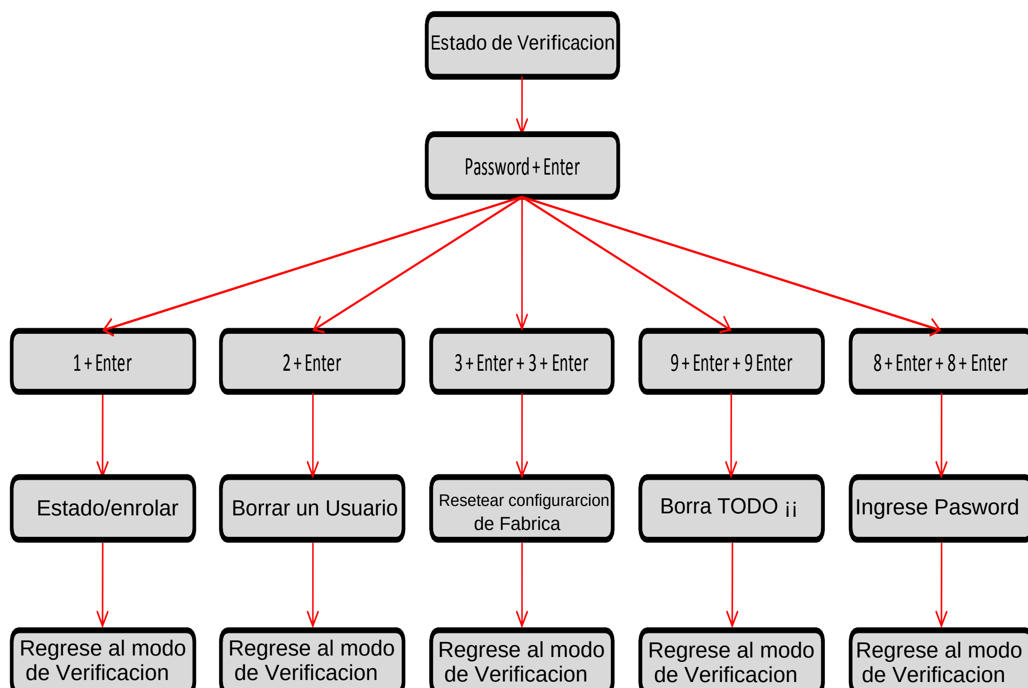
* pase su tarjeta 5 veces.

Tabla para borrar un solo usuario



3.2 Operación del Teclado USB

Tabla de operación con teclado



Sumario

* Proceso de borrado de un solo usuario

* Proceso con el teclado

3.2.1 Configurar Password para Teclado

Si el usuario necesita un teclado externo puede conectarlo directamente al aparato y solo pasar la tarjeta de administrador.
El sistema permite asignar un password al teclado.

Pasos de Operación:

- En el estado de verificación conecte el teclado con el dispositivo a través de USB
- Pase su tarjeta de admin para activarlo y se generara un comando que dirá --por favor presione el teclado--
- Escriba de "8" y pulse "Enter" A continuación, escriba "8" y pulse "Enter" de nuevo. El sistema generará el mensaje de voz: "Por favor, establecer una contraseña." Escriba su contraseña deseada y pulse la tecla "Enter". El sistema generará el mensaje de voz: "La operación se completó." Si no hay pulsaciones de tecla en 30 segundos, el sistema generará el indicador de voz: "Tiempo de la operación terminado. El sistema de volverá al modo de verificación". (la contraseña deberá ser de entre 4 y 6 dígitos)
- E l usuario podrá usar el teclado para la gestión de usuarios únicamente ingresando el password antes de usarlo, si este no detecta movimiento automáticamente se bloqueará.

1. Si se equivoca de password en seis ocasiones, El teclado se bloqueará y solo podrá ingresar de nuevo quitando la alimentación.

2. Si no hay actividad del teclado en 30 segundos este de descativará automáticamente.

3. El teclado deberá ser conectado despues de 15 segundos de otra manera el sistema no podrá identificar su estado.

3.2.2 Enrolar usuario mediante el teclado

Enrolar un usuario mediante el teclado externo es llamado **Modo de Enrolamiento base**. en este modo usted puede registrar un usuario con un número específico de ID

Pasos de Operación:

- Como se muestra 3.2 **Tabla de Operaciones de teclado USB** , escriba "1" y presione "Enter" para entrar al estado de enrolamiento.
- Cuando el sistema genera el comando "Registro de usuarios por favor ingrese el número de usuario." o entre el ID de usuario.
- El sistema generará el comando número**.Registro de usuarios por favor coloque el dedo o pase su tarjeta."(**indica el número de identificación del usuario. El sistema entra en el estado específico de inscripción ID.

Nota: si el usuario ya esta registrado con tarjeta se escuchará un comando que dirá --por favor coloque su dedo .

- Si el usuario esta registrado en el sistema como un usuario ID con 10 huellas se generará el comando: "Número de usuario **.por favor pase su tarjeta."
- En el estado de espera del ID de usuario registrado presione ESC para regresar al modo de verificación, si esto no responde presione ESC 2 veces para regresar al estado o modo de verificación

Nota: En el modo de enrolamiento con el teclado externo puede realizar los registros consecutivamente y el teclado regresara por si mismo la estado de modo de verificación por sí mismo.

Sumario

*Conecte el Teclado y pase su tarjeta para activarlo

* 8 + Enter + 8 + Enter

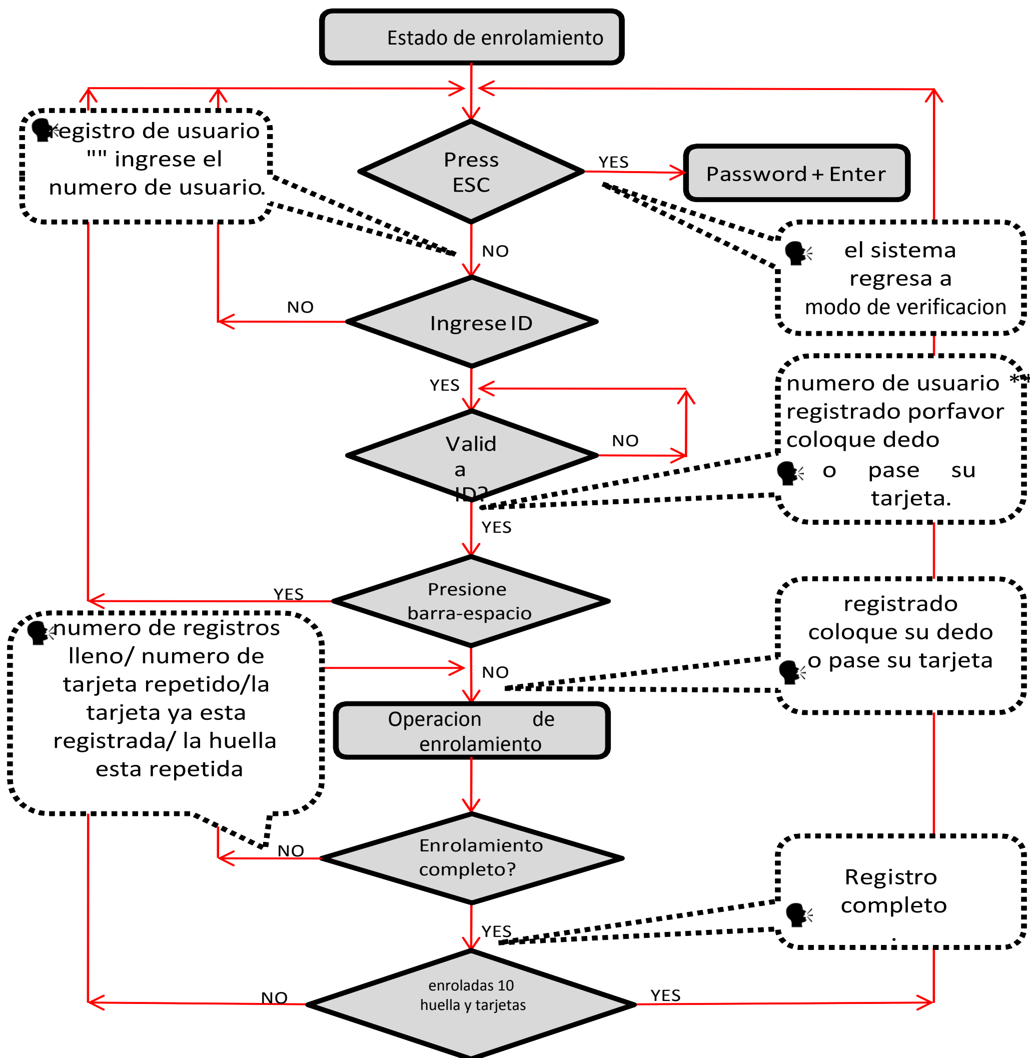
El tiempo de espera sera de solo 30 minutos

El password debera ser de entre 4 y 6 digitos

*Por favor Tome nota!!

*1 + enter estado de enrolamiento

Tabla de enrolamiento base con teclado:



Información Importante Adicional:

1. En el modo basado en teclado si los tiempos de efectuar cualquier operación sobrepasan el tiempo el sistema automáticamente le solicita esta operación una vez cada 10 segundos y vuelve al estado de verificación después de tres veces.

2. Las Huellas recién agregadas se sobrepondrán a las originales, basado en inscripción cualquier huella sobrescrita remplazara la antigua.

3. Un usuario sólo puede inscribirse con una sola tarjeta. Cuando el usuario se inscribe en una tarjeta del sistema, el sistema genera el mensaje de voz:"Por favor, pulse el dedo "Cuando el usuario pasa la tarjeta, el sistema genera el mensaje de voz: "La tarjeta ha sido registrada."

4. No se puede registrar un tarjeta dos veces de lo contrario el sistema generará el comando: "Tarjeta repetida." al pasar la tarjeta. Diferentes usuarios no pueden inscribir la misma huella, de lo contrario el sistema generará el indicador de voz: "La huella digital esta repetida". Durante el registro de huellas dactilares. Las nuevas huellas dactilares de un usuario siempre se sobreponen a las existentes.

La diferencia entre estos dos modos de inscripción de usuarios es cómo se vuelve al modo verificación.:

1.Con la tarjeta de administrador con un ID de usuario específico, el sistema vuelve al estado verificación después de que pase la tarjeta una vez.

2.Con el teclado solo será necesario el presionar en dos ocasiones la tecla ESC para que el sistema vuelva al modo de verificación, el mismo dirá el comando: "El sistema se encuentra en modo de verificación"

Sumario

* Proceso de enrolamiento con teclado

*El sistema le avisará 3 veces cada 10 segundos antes de volver al modo de verificación.

* No se pueden enrolar tarjetas repetidas.

* Pase su tarjeta solo una vez y el sistema volvera al modo de verificación

* ESC 2 veces y el sistema volvera al modo de verificacion.

3.2.3 Borrar un usuario especificado

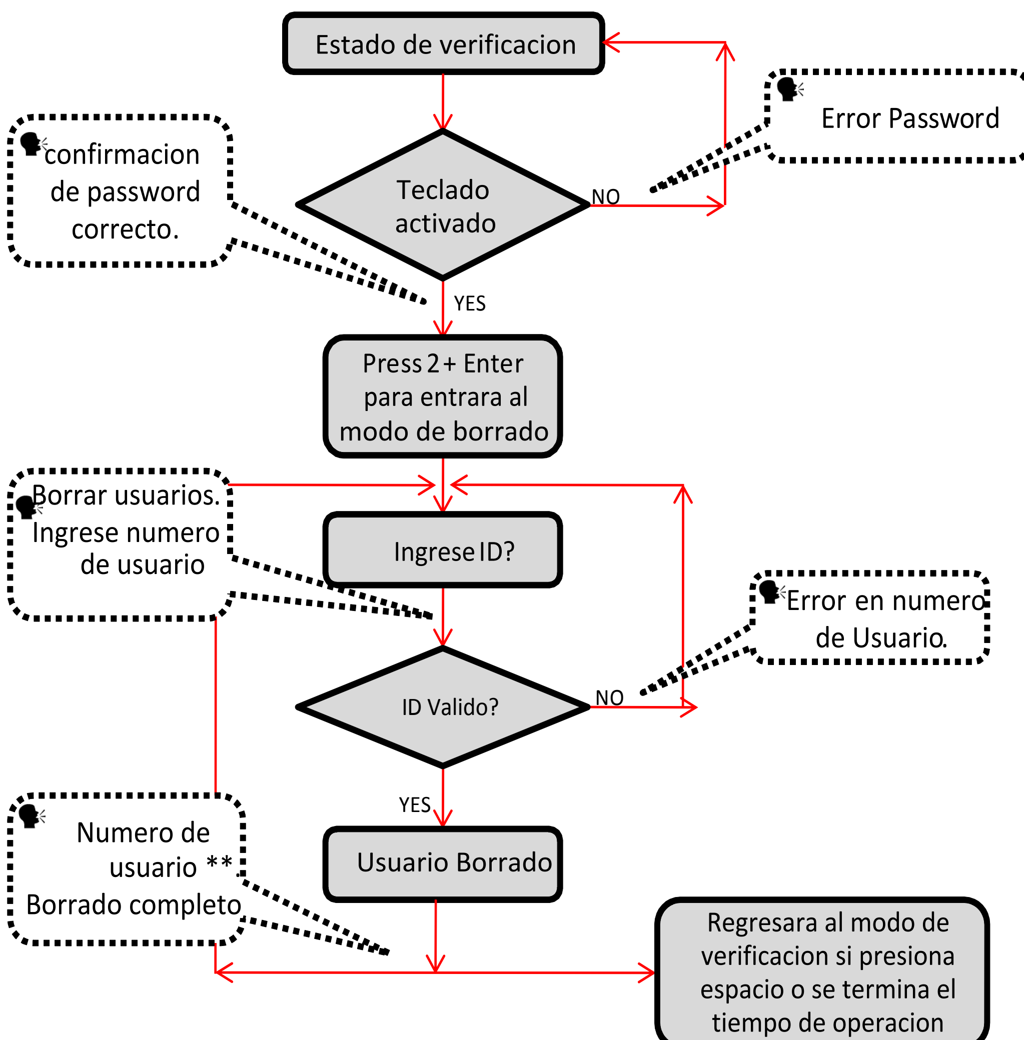
Borrando un usuario especificado con el teclado se llama **Borrado de usuario específico**.

Pasos de Operación:

- Conecte su teclado y pase la tarjeta de administración e ingrese el password si se cuenta con uno.
- Presione "2" y "Enter"; para entrar al modo de borrado de usuarios específicos, el sistema generará el comando: "Borrado de usuarios por favor agrega el número de usuario." y depués procederá al paso 3.
- Entre el número ID del usuario y este se encargará de checar y confirmar el proceso.
- Si el ID de usuario es válido, el sistema generará el indicador de voz: "Número del usuario. ** Borrado con éxito. Borrado de usuarios. Por favor, introduzca el número de usuario". Y automáticamente volverá al estado de borrado. Si el ID de usuario no es válido, el sistema generará el indicador de voz: "Error de número de usuario"
- Si presiona ESC" o rebasa el tiempo de operación el sistema automáticamente volverá al modo de verificación

Nota: En el modo de eliminación de un usuario específico el ID de usuario y ID de tarjeta de administración que están inscritos en el sistema se considerarán validos

- En el modo de borrado del teclado deshabilitará temporalmente la función del sensor de huellas o lector de tarjetas.



Sumario

* Conecte su teclado USB y pase su tarjeta para activarlo

* 2 + Enter ingresara al modo de borrado

* Ingrese el numero de ID

* Elsistema le confirmará el borrado de usuario.

*borre un usuario especifico

3.2.4 Borrando todos los USUARIOS

Pasos de Operación:

- Conecte su teclado y pase su tarjeta de administrador para activarlo
- Presione"9" + "Enter". después "9" + "Enter" de nuevo y se borraran los usuarios
- Si se logra con éxito el sistema dirá el siguiente comando: "Borrado de usuarios la operación a sido completada. El sistema vuelve al modo de verificación por favor registre la tarjeta de administrador"

 **Nota**: Usted puede borrar un administrador usando la función de borrar todo.

Puede también usar esta función parar borrar transacciones, usuarios y passwords.

Extreme precaución porque después de borrar toda esta información no habrá forma de recobrarla

3.2.5 Restablecer Valores de Fábrica

Pasos de Operación: Con teclado

- Conecte un teclado y actívelo pasando su tarjeta ingrese el password si se cuenta con uno.
- Presione "3" + "Enter". después presione "3" + "Enter" de nuevo y el sistema restablecerá los valores de fábrica.
- Después de la operación completada el sistema generará el comando: "Restablecer valores de fábrica completado. El sistema regresa al modo de verificación" usted también puede restablecer los valores de fábrica usando el tamper botton vea en 3.6 Botón Tamper, despues de que se han restablecido los valores toda la información será reiniciada de fábrica, incluyendo ID, password, dirección IP, Dirección RS485 y password de teclado.

Sin el Teclado:

- Desconecte la alimentación, presione y mantenga el BOTON TAMPER . después que regrese la alimentación espere por el comando de voz después suelte el botón y espere 40 segundos, después presione el botón 3 veces y el relay se activará 3 veces y solo lo suelta al final. Repítalo si no funciona a la primera.

 **Nota**: La información de los usuarios así como ellos mismos no serán borrados

3.3 Funciones de Control de Acceso

3.3.1 Funciones de Control de Acceso

Configuración de Control de Acceso es para que los usuarios abran puertas en zonas de tiempo y el equipo controle parámetros para la apertura de electroimanes.

Para abrir, el usuario debe cumplir con las siguientes condiciones:

- La hora actual debe coincidir al acceso de la zona horaria del usuario o el uso horario de acceso al grupo que él / ella pertenece .
- El grupo en el que el usuario debe estar será una de las combinaciones de desbloqueo. El primer grupo es el grupo por defecto para todos los nuevos usuarios. El grupo en el que el usuario debe ser es el control de acceso / grupo de combinación de desbloqueo (unlock) (el usuario puede modificar el ajuste correspondiente de control de acceso, a través del software de control de acceso).

 Nota: La función de control de acceso del dispositivo será necesario establecerla y modificarla a través del software de control de acceso, para los detalles, por favor consulte el manual de usuario del software.

Sumario

* Conecte su teclado y pase su tarjeta para activarlo

* 9 + Enter + 9 + Enter y se borraran todos los usuarios

* Recuerde que todo lo borrado ya no podra ser restablecido.

* 3 + Enter + 3 + Enter - restablece valores de fabrica

* Restablecer valores de fabrica no borrara usuarios.

* El sistema por defaul es grupo y zona de tiempo 1.

* El usuario opuede modificarlas mediante el software.

3.3.1 Funciones de Control de Acceso

La configuración de Control de Acceso para que el usuario abra la puerta en una zona de tiempo específica controlando los parámetros del electroimán

Para abrir el usuario registrado debe cumplir con las siguientes condiciones:

- El tiempo de apertura debe coincidir con la zona de tiempo establecída y el grupo de acceso.
- El grupo donde el usuario esté debe estar en el control de acceso (o del mismo control de acceso de un grupo para abrir la puerta juntos). El sistema por defecto abrirá la zona por default del grupo, usted puede agregar o modificar las zonas de tiempo para los grupos desde el software.

✍ Nota: Las zonas de tiempo en el equipo deben ser creadas y modificadas desde el software y después transmitidas a este, se recomienda crearlas primero antes de agregar usuarios

1. Zonas de Tiempo de Control de Acceso:

Las zonas de tiempo son las unidades mínimas para el acceso de un usuario, estas podrán ser creadas desde el software y agregadas por usuarios, también pueden agregarlas a los grupos y agregar un usuario a este grupo, el sistema le brindara la zona de tiempo del grupo por default.

2.Configuración de Acceso días Festivos

Este tiempo de control de acceso especial tal vez sea necesario durante las vacaciones. Es difícil modificar el tiempo de control de acceso de cada persona. Así que se recomienda revisar directamente el manual del software para realizar esta función.

3. Acceso de Grupos con Zonas de Tiempo:

Agrupando y gestionando grupos. Los empleados agregados en grupos usarán las zonas de tiempo de estos grupos por default de hecho a cada empleado de este grupo también se le puede configurar una zona, los grupos siempre mantendrán sus zonas, la opción siempre existirá de agregar un nuevo usuario a diferentes grupos.

4. Configuración de Combinación de desbloqueo (UNLOCK) :

Para mejorar el nivel de seguridad puede utilizar esta función. Para abrir la puerta, se necesitan 5 personas diferentes de 5 grupos diferentes, lo que significa que la puerta no se puede abrir a menos que las 5 personas hayan pasado el proceso de verificación.

5. Parámetros de Control de Acceso:

Retardo de Control de Bloqueo (lock control delay): Se aplica para determinar el tiempo de desbloqueo, la unidad de medida mínima es de 20ms, en condiciones normales es de 100-200ms.

Anti-Passback: Configurable a "Nada", "salir ", "entrar", "entrar/salir".

Estado de Registro del Maestro: Configurable a "nada", "salir", "entrar".

Modo del sensor: Este modo puede configurarse a "nada", "Normalmente abierto (NOpen)", "Normalmente Cerrado (NClose)"

Retardo del sensor (Sensor Delay): Configura el retardo del sensor después de que la puerta fue abierta, si la puerta no está cerrada dentro del tiempo de retardo del sensor, se activa la alarma. El rango de dispositivos de pantalla blanco y negro es 0-254 y dispositivo de pantalla a color es de 0-99.

Sensor de Alarma: Configure el tiempo de retardo de la alarma, después de la activación de esta se disparara configurable a un rango de 0-999 segundos.

Tiempo de Errores de Alarma: Definir los tiempos de error máximo para activar la alarma. Cuando no se pasa la cautela de verificación y exceden los tiempos definidos, la señal de alarma se activará automáticamente.

6. Configuración de Anti-Pass back:

Función de Anti-Pass back, por favor revise 4.2 Anti-Pass back.

7. Deshabilitar Alarma: (Tipo de alarma: Alarma de puerta y Alarma de tamper). Cuando el dispositivo esta en estado de alarma, la verificación del usuario puede desactivar la alarma y este volverá a su estado normal o de lo contrario se activara nuevamente.

Sumario

* La zona de tiempo por defaul es la 1.

* El usuario puede modificarlas desde el software.

* 50 zonas de tiempo por unidad

* Cada usuario puede pertenecer a tres

* La configuracion de zonas de tiempo en dias festivos se pueden aplicara a los usuarios.

* El usuario puede pertenecer a un grupo y este grupo tendra su propia zona de tiempo.

* Modo de Control del Iman

* Anti-passback

* Modo de Sensor

* Sensor de Alarma

* Tiempo de Errores de Alarma

3.4 Verificación de usuarios

La verificación por default en el equipo es FPy RF, puede modificar este modo de verificación desde el software como RF o FP al igual que RF+FP o solo uno de estos dos, para mayor información visite el manual del software.

Pasos de Operación:

- Cuando el equipo esta en el modo de verificación, el sistema dira el comando: “Verificación de usuario por favor pase su dedo o coloque su tarjeta"
- Comenzará la verificación de usuarios. El equipo soporta 4 modos diferentes de verificación usuarios: FP/RF, FP, RF y FP&RF .

- **Verificación Fingerprint/Huella (FP)**

Solo presione su dedo en forma plana en el sensor, si la verificación es correcta el sistema pronunciara el comando: “Número de usuario**. Gracias.” y después brindará el acceso, si la verificación falla el sistema pronunciará el comando: “Coloque su dedo otra vez.”

- **Verificación con Tarjeta**

Solo pase su tarjeta por el área recomendada, si el acceso es correcto el sistema pronunciará el siguiente comando: “Número de usuario **. gracias.” y le brindara el acceso pero si la verificación falla el sistema pronunciará el siguiente comando: "Por favor pase su tarjeta otra vez"

- **Verificación con Fingerprint/Huella + Tarjeta**

Configure el modo primero a FP & RF desde el software, la operación de la verificación será la siguiente:

- **Coloque el dedo Primero**:

Coloque el dedo en la forma apropiada y si la verificación fué correcta el sistema dirá el comando: “Número de usuario **, por favor pase su tarjeta”. Después será brindado el acceso si la verificación falla el sistema generará el comando: "Por favor pase su tarjeta de nuevo".

- **Pase la Tarjeta primero**

Pase su tarjeta por el área recomendada si la verificación es correcta, el sistema generará el comando: “Número de usuario **, por favor coloque su dedo”. Si todo es correcto brindará el acceso, si el modo de verificación falla, el sistema generará el siguiente comando: “Por favor coloque su dedo otra vez.”

- **Verificación de Huella o Tarjeta**

Este es solo un modo de verificación (1) de (2) a escoger.

Tip: Si el usuario no cuenta con un a zona de acceso valida el sistema generará el comando: "Zona de acceso invalida".

- Si el usuario no usa el modo de verificación que se le a otorgado no podrá acceder y el sistema generará el comando: “Modo de verificación invalido.”

Sumario

* FP = fingerprint (huella)
* RF = Acces card (Tarjeta)

* 4 modos de verificacion

** FP / RF, FP, RF & FP&RF como verificacion

* Configure el modo de verificacion desde le software

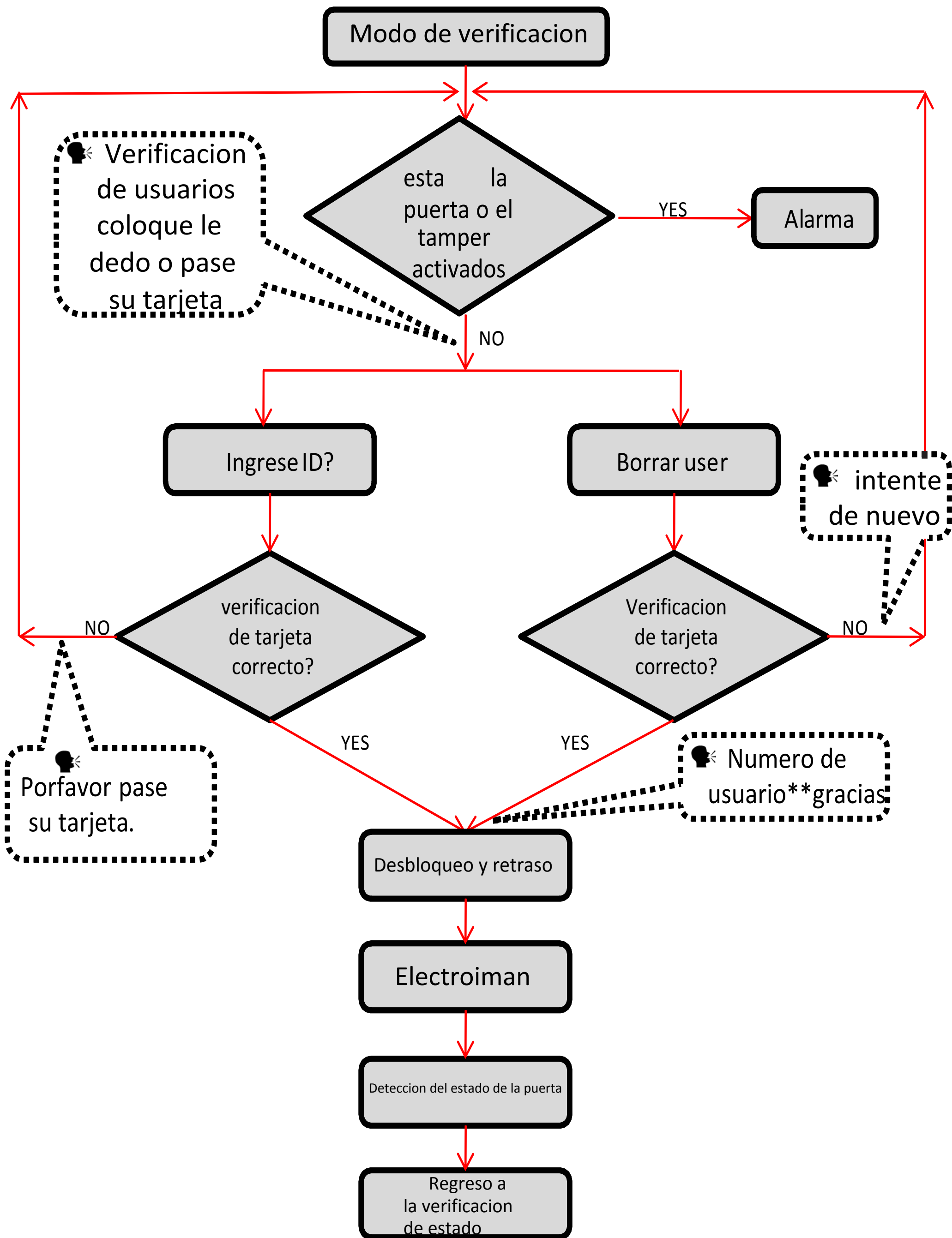
* FP primero y luego RF

* RF primero y luego FP

* FP o RF

* Tabla de verificacion de usuario

Tabla de Verificacion de usuarios:



3.5 Memoria USB

El usuario puede descargar reportes, descargar usuarios, subir usuarios y actualizar el firmware del equipo mediante la memoria USB.

- **Descargar Reportes**: Descargue los reportes de asistencia de todos los usuarios con la memoria USB.
- **Descarga de usuarios**: Descargue los usuarios con su información incluyendo los templates de las huellas digitales de los mismos
- **Subir Usuarios**: Suba información de usuarios con memoria USB al equipo.
- **Actualice Firmware**: La actualización del firmware mediante la USB.

La creación y modifiación de estos archivos puede ser realizada usando el software de control de acceso para referencia revisa el manual del software.

✍ **Noticia**: Por favor no actualice los firmwares a discreción porque puede crear un daño irreversible a los equipos, recuerde que cada firmware es creado para un equipo en específico, no puede ser instalado en otros aunque sean el mismo modelo.

La Operación de USB incluye cualquiera de los siguientes casos:

- Si conecta la memoria USB el sistema automáticamente le brindará los comandos de seguimiento para la secuencia de configuración del equipo.
- Después de conectar la USB en el equipo pase su tarjeta para entrar al modo de gestión de memoria USB (U-DISK).
- El sistema generará el comando: "****. Por favor pase su tarjeta de administrador para confirmar." (**** indica las cuatro posiciones de trabajo de A a D en la secuencia, lo mismo más adelante)
- Si quiere modificar la gestión de USB, confirme con su tarjeta si la operación esta completa, el sistema generará el comando: "Operación completada" y podrá pasar al siguiente paso, al finalizar con los cuatro pasos el sistema generará el comando: "El sistema regresa al modo de verificación". Si la operación falla, este generará el comando: "La operación falló, el sistema vuelve a modo de verificación.
- Si no pasa la tarjeta de administrador el sistema automáticamente saltará los pasos después de 5 segundos y lo enviará al siguiente paso. al termino de los cuatro pasos el sistema regresará al modo de verificación automáticamente.
- Si usted conecta una memoria USB que ya ha sido configurada en el equipo, al conectarla este respetará las configuraciones ya estipuladas.
- Después de conectar la memoria USB en el equipo solo es necesario pasar su tarjeta para entrar al modo de gestión de USB (U_DISK).
- El sistema obtiene los comandos de operación del USB leyendo un archivo en esta misma, después generará el comando: "Leyendo configuración de memoria (U_DISK) pase su tarjeta para confirmar."
- Después de pasar su tarjeta y realizar las operaciones el sistema generara el comando: " ****. Operación completada." así mismo al término de cada secuencia si alguna de estas falla escuchara el comando: " ****. La operación a fallado."
- Después de terminar con la operacion el sistema generarar el comando: "El sistema regresa al modo de verificación".

✍ **Nota**: Por favor, espere 8 segundos después de insertar la USB en el dispositivo, de lo contrario, el sistema no puede detectarlo correctamente.

Sumario

* Descarga de reporte

* Descarga de Usuarios

* Subir Usuarios

* Actualizar Firmware

* Conecte la USB y pase su tarjeta para activarla

* Si no toma accion en 5 segundos el sistema saltara los procesos y regresara a su modo normal.

*Si la configuracion ya existe el sistema se lo cofirmara.

3.6 Botón de Sabotaje (tamper)

Se presiona el interruptor de sabotaje manteniéndolo así con la base trasera. Cuando se desmonta el dispositivo el interruptor de seguridad se levantará y luego se enviará una señal de alarma para activar una alarma externa.

Reconocer Alarma: Puede desactivar la alarma de sabotaje abriendo la puerta con una verificación correcta de usuarios registrados.

Restablecer Valores de Fábrica: los valores de fábrica pueden ser restablecidos con el mismo botón de sabotaje

Cuando el sistema genere una alarma por 30–60 segundos el usuario puede presionar el botón tres veces (escuchara un beep) para restablecer los valores, incluyendo número de equipo, password del sistema, Dirección IP, dirección 485 y password de teclado externo

✍ **Nota**:

Toda la información de usuarios NO será borrada después de restablecer los valores de fábrica.

Los valores de fábrica pueden ser restablecidos incluso usando el teclado externos, vea 3.2.5 restablecer valores de fábrica.

Sumario

* Este Tamper se encuentra en la parte trasera del equipo y debera estar presionado todo el tiempo.

* Cuando este sea activado se activara la señal de alarma

* Con la alrma activada suelte el tamper y presionelo en tres ocaciones despues de esperar entre 30 a 60 seg.

4.0 Apéndice A

- Lista de parametros

* Lista de parametros

Características

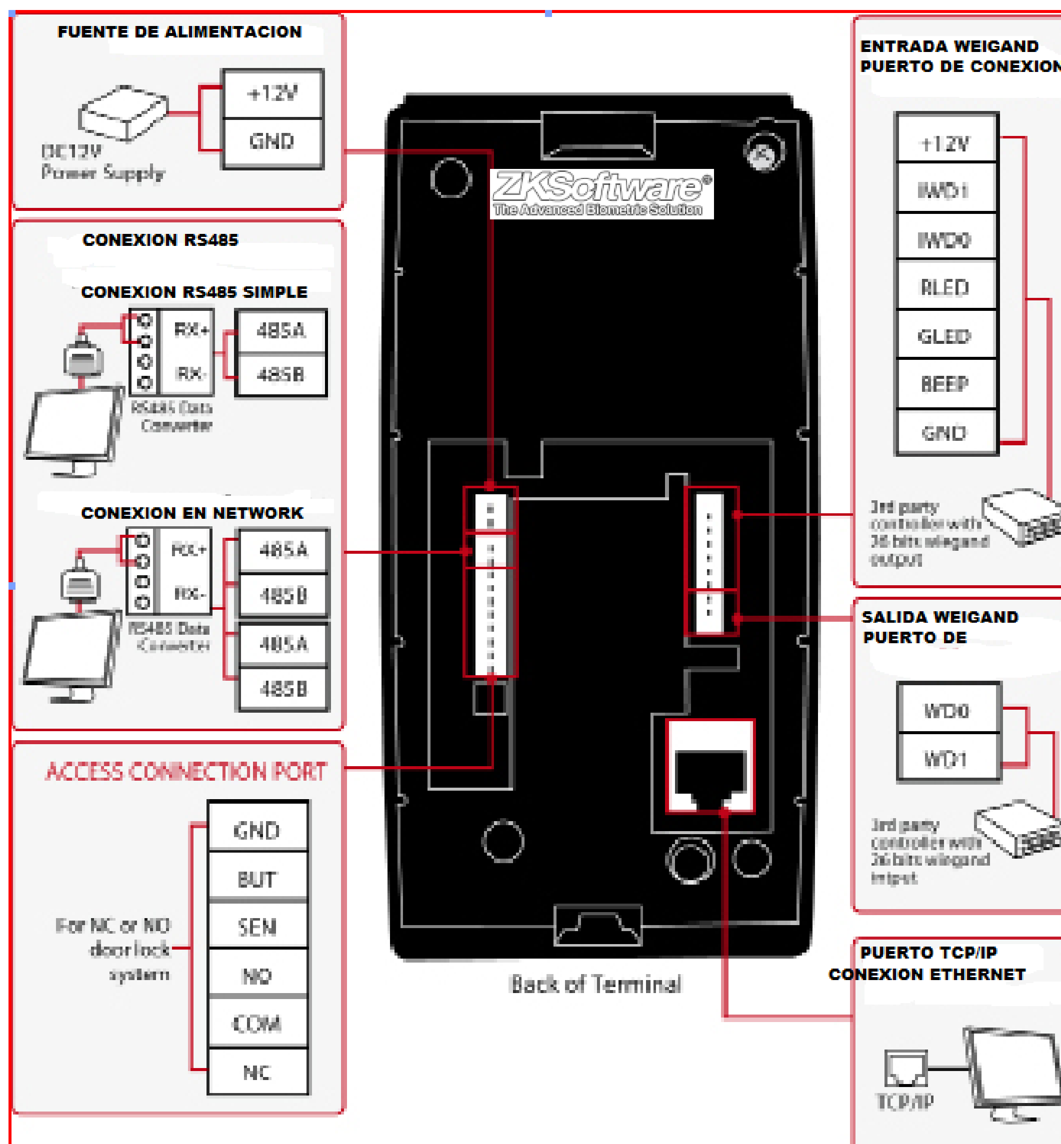
- Reliable, durable and highly accurate ZK optical sensor
- IP54 Rated metal casing
- Less than 1 second user recognition
- Stores 1,500 templates, 10 000 cards and 50,000 transactions
- Reads Fingerprint and/or RFID card
- Supports 50 time zones, 5 groups and 10 unlock combinations
- Integrated 125kHz RFID proximity reader
- Built-in Serial and Ethernet ports
- Built-in Wiegand input/output ports for connection to third party control panels
- Built-in USB port allows for manual data transfer
- Audio - Visual indications for acceptance and rejection of valid/ invalid fingers
- Tamper switch

Especificaciones

Fingerprint Capacity:	1,500 templates
Transaction Capacity:	50,000 transactions
RFID Card Capacity:	10,000 cards
Hardware Platform:	ZEM710
Sensor:	ZK Optical Sensor
Algorithm Version:	ZK Finger v10.0
Built-in Card Reader:	125kHz RFID proximity reader
Communication:	RS485, TCP/IP, USB-host
Wiegand Ports:	Input and Output any bits
Access Control interfaces:	3rd party electric lock, door sensor, exit button, open door alarm.
Access Control functions:	50 time zones, 5 access control groups, 10 unlock combinations.
Power Supply:	12V DC 2A
Operating Temperature:	-10 ˚C - 60 ˚C
Operating Humidity:	10%-90%
Dimension:	73X148X34.5 mm

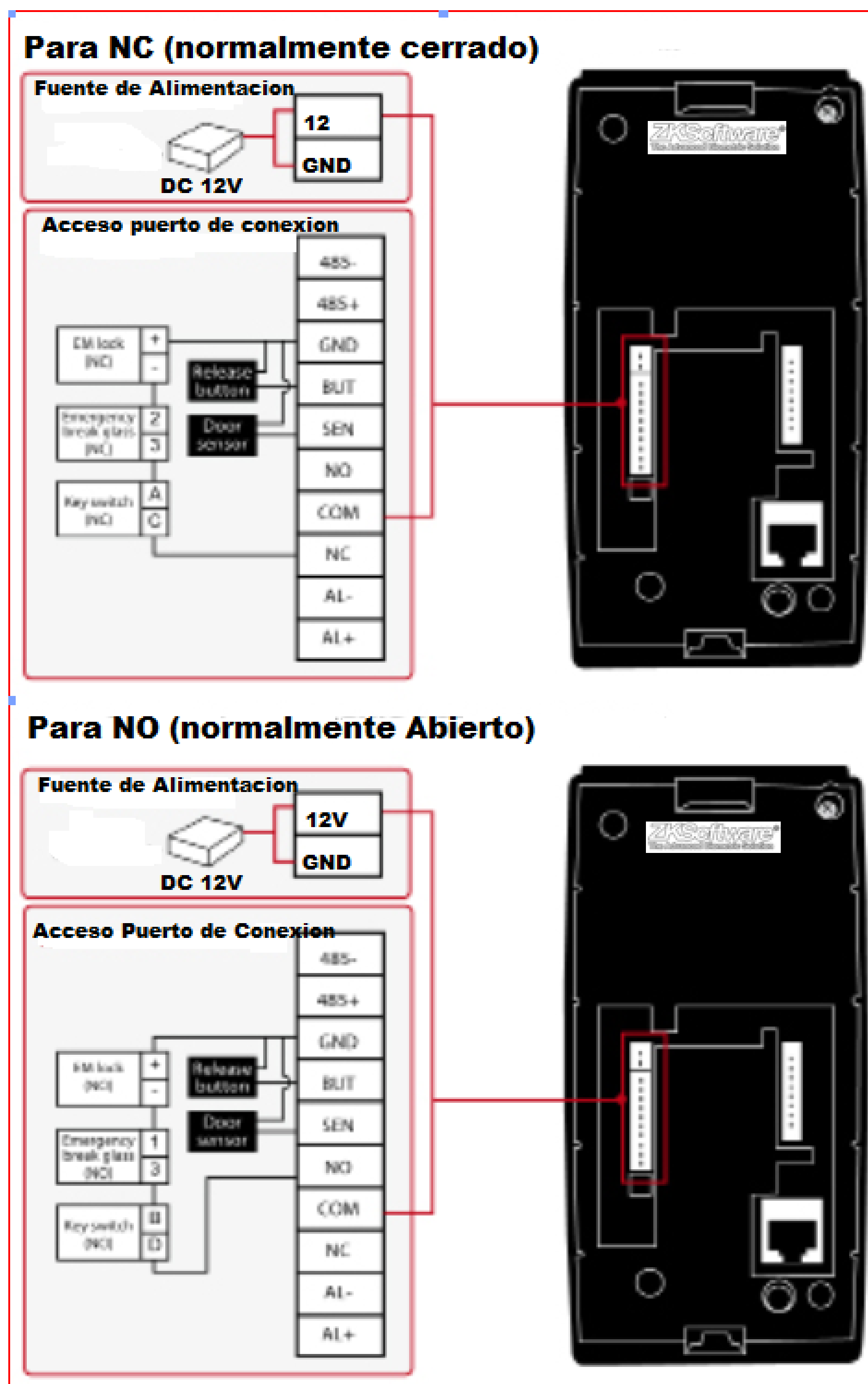
4.0 Apéndice B

Diagarama de cableado para la conexión de puntos de alimentación y comunicación



6.0 Apéndice C

•Diagrama de cableado para NO (normal/abierto) & NC (normal/cerrado) Sistema de cerrado de la puerta



Apéndice A:

Plugs de Salida del MA300

Terminal	Función
+ 12V	Entrada Alimentación
GND	Entrada Alimentación
485 -	RS 485
485 +	RS 485
GND	Botton / Sensor/puerta
BUT	Botton / Sensor/puerta
SEN	Sensor/puerta
NO	Electro Imán
COM 1	Electro Imán
NC	Electro Imán
AL -	Alarma
AL +	Alarma

Terminal	Función
+ 12	Salida Alimentación
IWD 0	Entrada Wiegand
IWD 1	Entrada Wiegand
RLED	Entrada Wiegand
GLED	Salida
BEEP	Salida
GND	Salida
WD 0	Salida Weigand
WD 1	Salida Weigand

